NASA/TM-20220004794

Federal Unmanned Aircraft Systems Traffic Management

Concept and Joint Evaluation with the Department of Defense

Abhay R. Borade
Ames Research Center
Moffett Field, CA

Jeffrey R. Homola
Ames Research Center
Moffett Field, CA

Joseph L. Rios
Ames Research Center
Moffett Field, CA

Cynthia A. Wolter
San Jose State University Research Foundation at Ames Research Center
Moffett Field, CA

National Aeronautics and
Space Administration

October 2022

NASA STI Program . . . in Profile

Since its founding, NASA has been dedicated to theadvancement of aeronautics and space science. The NASA scientific and technical information (STI) program plays a key part in helping NASA maintainthis important role.

The NASA STI program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NTRS Registered and its public interface, the NASA Technical Reports Server, thus providing one of the largest collections of aeronautical and space science STI inthe world. Results are published in both non-NASAchannels and by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phaseof research that present the results of NASA Programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.
- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or ofspecialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.
- CONTRACTOR REPORT. Scientific andtechnical findings by NASA-sponsored contractors and grantees.
- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars,or other meetings sponsored or co-sponsored by NASA.
- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions,often concerned with subjects having substantial public interest.
- TECHNICAL TRANSLATION.

  English-language translations of foreign scientific and technical material pertinent toNASA's mission.

Specialized services also include organizing and publishing research results, distributing specialized research announcements and feeds, providing information desk and personal searchsupport, and enabling data exchange services.

For more information about the NASA STIprogram, see the following:

- E-mail your question to help@sti.nasa.gov
- Phone the NASA STI Information Desk at 757-864-9658
- Write to:
  NASA STI Information Desk
  Mail Stop 148
  NASA Langley Research Center
  Hampton, VA 23681-2199

Acknowledgements

This effort required collaboration across many groups and individuals within NASA. Sherry Jurcak, Mark Rossner, Jinn-hwei Cheng, Abhinay Tiwari, Sung Hoon Ko, and Priya Venkatesan gave their software engineering expertise to develop the systems tested in the field. Sherry provided further invaluable assistance through her on-site technical support of all the fielded NASA systems. David Smith, Madison Goodyear, and Madhavi Latha Balijepalle provided additional technical support to make the test preparation and execution successful. Paul Liu tied the team together with vital systems engineering insights. Parimal Kopardekar and Anna Cavolowsky helped develop and execute the project from the NASA Aeronautics Research Institute (NARI). Without this full team's effort, this research could not have been successful.

Table of Contents

Table of Figures

Table of Tables

Federal Unmanned Aircraft Systems Traffic Management
Concept and Joint Evaluation with the Department of Defense

Abhay R. Borade, Jeffrey R. Homola, Joseph L. Rios
NASA Ames Research Center
Cynthia A. Wolter
San Jose State University Foundation at NASA Ames Research Center

Introduction

There has been growing demand for the use of small Unmanned Aircraft Systems (UAS) domestically and globally. The versatility of vehicles to support many use cases and business models with broad advances in technology has created an industry with clear growth and continued growth potential. However, an early barrier to operations at scale has been the lack of a coordinated airspace management approach. To address that barrier, NASA pioneered a revolutionary airspace management paradigm that incorporated a federated, service-based approach to enable fair, safe, and scalable operations of small UAS in the nation's airspace. This paradigm came to be known as UAS Traffic Management (UTM) [1]. During the UTM Project, NASA worked closely with the Federal Aviation Administration (FAA) and Industry to develop a system and supporting concept that incorporated the needs and perspectives of Industry and balanced them with the regulatory and operational needs of the FAA. Through development and rigorous testing, NASA evolved and strengthened the UTM concept and associated system architecture hand-in-hand with partners and stakeholders, which has gone on to take hold globally and move forward toward dedicated implementation in the US through rulemaking and standards bodies.

A fundamental aspect of UTM is the sharing of information by operators through data exchanges supported by services. A core service element of the architecture that supports these data exchanges is referred to as a UAS Service Supplier (USS) [2]. Operators subscribe to a USS, which can assist with operations planning based on data exchanges with other USSs to build a common picture of the airspace and the necessary situation awareness to operate in the presence of others and the constraints of the airspace.

With the growth in use of small UAS in the United States and further maturation of UTM, there has been a demand for Federal Agencies to take part in the UTM ecosystem. With this demand comes the need to develop a Federal UAS Service Supplier (FUSS) that will allow agencies to participate, observe, and act with commercial and private operators while accounting for the unique needs and requirements of each agency. The requirements for a FUSS will be dependent on the agency, its mission, and available assets. The need for UTM has grown to include government participation ranging from local sites, fire, police, to search and rescue, and now Federal Agencies. However, NASA's current concept will initially focus on the Department of Defense (DoD) and the Department of Homeland Security (DHS) with their specific needs regarding the development of a common operating picture for their operators and personnel through role-based access, the integration of Counter UAS (C-UAS) assets and capabilities, and USS messaging.

Current Security Operations & Gaps

Currently the DoD has Air Traffic Control (ATC), C-UAS, and UAS operators that operate on separate platforms. This structure has the potential to create a lag in communication and reduction in overall situational awareness and operational effectiveness. For example, a UAS operator in the field may have phone communication with ATC while the C-UAS operator has a separate direct line with ATC. Under such organization, by the time a C-UAS operator was able to detect a potential threat, communicate with ATC, who in turn would potentially get in touch with a friendly UAS crew, it could be too late before a threat was to intrude in protected airspace. This type of communications gap would be addressed through the implementation of a common platform for security users to communicate through and to build an awareness of the airspace situation based on shared information and access.

Situation awareness for all Participating and Non-Participating operations

To build common situation awareness and address potential communications gaps from a security perspective, UAS operations can be simplified into two categories: Participating or Non-Participating with regards to UTM. A Participating operation is one in which the operator is acting in compliance with the rules and regulations of the airspace in which the vehicle is flying, the operation is supported by a USS and discoverable to others in the system, and the operation is identifiable on demand. A Non-Participating operation is one that is not operating in accordance with the above characteristics and presents a potential challenge to others in the airspace and to those protecting assets. The classification of an operation as being either Participating or Non-Participating is a streamlined first step in a decision tree that dictates potential threat responses and mitigations.

Identified needs from DoD for small UAS support and integration with UTM

To begin the task of assessing and acting upon the needs for UAS support and integration with UTM, security agencies have identified the following assumptions, guidelines, and parameters for UAS operations and the various associated stakeholders:

1. Participating in Contiguous United States (CONUS) UAS operations
2. Having awareness of Commercial UAS operations
3. Limiting certain DoD operations from being shared with the public or other agencies
4. Improving communication between ATC and UAS operators
5. Create instant communication between ATC and C-UAS operators
6. Create interagency messaging to facilitate coordination between FUSS users

These guidelines provide a strong foundation for developing the basis for a FUSS and a Common Operating Picture (COP) to inform the different actors and stakeholders across roles in a standardized, actionable format.

Approach to Solutions and Test Objectives

The identification of initial FUSS requirements and operational needs were a product of early engagement between NASA and security agencies. Based on this engagement, NASA conducted an initial simulation of UTM with a security focus followed by integrated flight testing with security and commercial operations in a UTM environment. Building upon this successful demonstration, the evolution of the Federal UTM concept continued with a more refined focus on enabling and promoting common situation awareness, providing role-based access to

information, facilitating information exchange between operators via a common messaging framework, and the implementation of UAS operation categorization based on sensitivity level and handled accordingly by the FUSS. A NASA-led flight test involving security agencies and partners was planned and executed to demonstrate these focus areas. The primary research participants in this testing included NASA Ames Research Center, the Collaborative Low Altitude UAS Integrated Effort (CLUE), The Northern Plains UAS Test Site (NPUASTS), the DoD, and the DHS.

The following objectives were accomplished:

- Tested 3 scenarios that allowed Federal operators to use UTM for their own flight planning, as well as design and integrate UTM into a Federal COP
- Created role-based access for Federal personnel, specifically for an Air Traffic Controller and Counter-UAS operator. These personnel were able to log into the Common operating picture and use the integrated UTM, C-UAS, and sensor data to inform decision making
- Tested messaging between Federal operators in the field and other personnel such as ATC, C-UAS, Manned pilots, and UAS crews
- Tested 3 categories of mission types: Non-Sensitive, Sensitive, and Sensitive Protected. Each type of mission would share or not share certain UTM data based on the type of mission.

NASA Test Components

Architecture: USS and DSS

To enable federated traffic management via a collection of automation-enabled entities, those entities require a way to discover how to connect with each other. NASA tested approaches to this discovery process during its flight testing [3] and then industry developed improved approaches, including one called Discovery and Synchronization Service (DSS). DSS is currently being developed to meet the requirements of emerging standards [4]. DSS was tested in various forms during NASA flight testing [5], [6], FAA flight testing [7], [8], and other international flight test events.

DSS works like an "intelligent phonebook[1]" by allowing an authorized component, like a service supplier, to indicate that relevant data for a particular geography and time exist and can be queried from that service supplier. By design, the DSS does not hold operational details, rather it holds pointers to authorized entities that manage operational details. In addition to this discovery mechanism for relevant data, the DSS acts as a synchronization mechanism to eliminate race conditions between the various stakeholders. The DSS acts as a single-source-of-truth for shared data and arbitrates the order in which data are submitted or known to the system as a whole.

Per the design and concept of DSS, in any given geographic region there is expected to be a single logical DSS. However, the design of DSS allows it to be supported by multiple organizations in a distributed manner with data submitted to any particular instance of DSS made eventually consistent [9], [10] across all instances of that DSS deployment for that geographic region. For example, in Figure 1 below, a collection of UAS Service Suppliers (USS) each use a commercially supplied DSS for discovering each other and synchronizing certain data. The Commercial DSS works logically as a singular system. However, that DSS is actually a collection of providers coordinating to maintain a cohesive view of the shared data, with some

[1] https://sn.astm.org/?q=features/drones-move-mainstream-ja20.html

providers potentially providing multiple instances. In some deployments a single organization may be DSS Provider as well as a USS, but the roles are defined distinctly.

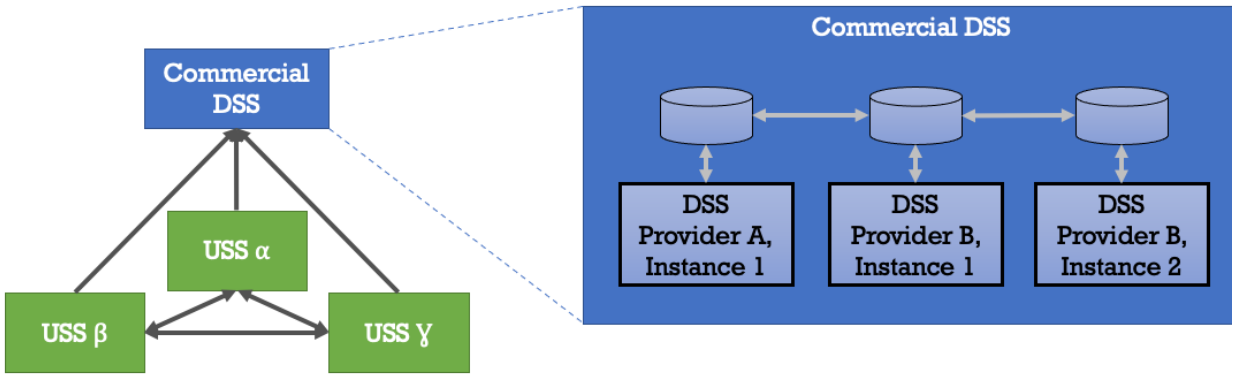

Figure 1. *Example of commercial Discovery and Synchronization Service (DSS) architecture*

A commercial DSS deployed as currently envisioned by industry and NASA for future Beyond Visual Line of Sight (BVLOS) operations has several drawbacks for security and defense purposes.

1. Data submitted to a commercial DSS is visible to DSS Providers regardless of any additional access measures applied to reading or writing to that commercial DSS.
2. Authorization to the commercial DSS is managed by an organization other than the security or defense stakeholders.
3. A commercial DSS is reliant on the various providers to maintain availability, performance, and other non-functional qualities of the system without any current contractual mechanism to guarantee those qualities.

It is this set of drawbacks that led NASA to propose an updated architecture to support security and defense stakeholders. An additional DSS for sensitive data could alleviate the three drawbacks listed above. There are other solutions possible that address one or two of the drawbacks, but after discussion with subject matter experts at NASA and participants of the flight test, this architectural solution was the most complete to cover use cases. This additional DSS could be called a “Security DSS” which is deployed directly by a security or defense organization or by an entity designated by those organizations.

One note on this approach is that it assumes there is a level of sharing that must occur between recognized organizations. If a single organization needs to manage its own operations and does not want nor need to share operational data with other independent organizations, then there is no express need for a DSS. Everything that can be “discovered” or “synchronized” can be handled by a single USS.

A system with two DSSs requires further definition of protocols for those subjects that have access to both DSSs. For commercial operators that already have access to the commercially provided DSS, they would not need to access the Security DSS, so their workflows would not need to change. For security agencies that do have access to the Security DSS, new protocols for when they would need to use one or the other (or both) DSSs is required. For example, the DoD may have non-sensitive operations that operate collaboratively with commercial USSs. These operations would share data in the same manner that those commercial operations do via the DoD’s USS. Certain sensitive operations that need to be shared with another security agency like DHS, would need to use the Security DSS to do so. The same data exchange protocols are leveraged, but the network and services are restricted to use by the authorized security organizations. Commercial USSs and operators would not have access to these data.

A deployment of such a double DSS system may resemble what is presented in Figure 2, which is also the configuration developed and used in support of the described flight activity. Note that the codebase for both DSS is identical. Only the configuration and deployment environments were different. The fact that the DSS is open source and provided by industry via the Linux Foundation has great value to government operations. Government systems can remain compatible with industry standards, yet still have a controlled deployment of the same software when necessary.

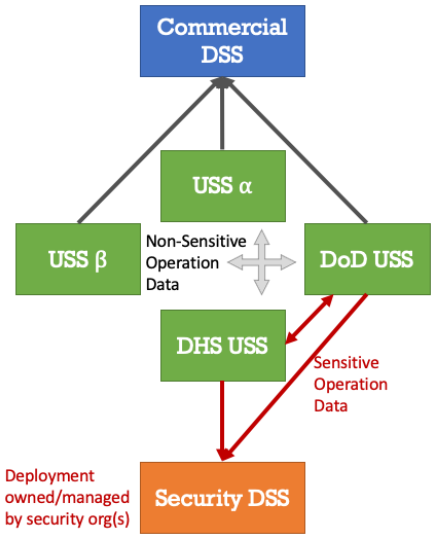

Figure 2. *Addition of Security DSS to connect Federal USSs supporting sensitive operations and limit sharing of sensitive information while allowing for non-sensitive operations within the commercial UTM environment*

A major design decision in this configuration is what authorization servers are going to be recognized by the Security DSS. At a high level, an authorization server provides tokens to actors to secure communications between those actors in the system. For example, for USS A to talk to USS B, USS A would request a token with appropriate scopes from the authorization server (Figure 2). USS A would have to authenticate to that authorization server and the tokens requested would have to be allowed per the Role-Based Access Control (RBAC) rules that have been established. When USS A obtains that authorization token, it can then use that token to exchange data with USS B. This configuration established for this test activity leveraged the OAuth 2.0 standard [11]. For a deeper dive on how authorization and authentication are expected to work in the UTM environment, see [12].

There are two primary options for authorizing communications with the Security DSS and amongst the security-focused USSs:

1. Use the same authorization server as used with the Commercial DSS and USSs
2. Deploy an additional authorization server to facilitate security-focused communications.

In recent field tests of UTM [5], [6], [7], [8], a system called FIMS-Authz was deployed by an entity playing the role of the FAA in a future scenario wherein the FAA provides such a service. It may be that some other entity is recognized to provide authorization services in the future. If the FAA is providing the service and DoD and DHS are regularly using it in order to communicate non-sensitive operational data with commercial users, then it is trivial from a technical perspective to also use it for securing communications within the security context. However, there is a major issue that would need to be explored before operationalizing this

approach: Does a token request that will be used for communications about sensitive operations contain any information that should not be shared with a non-security organization server?

Depending on the interface and Role-Based Access Control (RBAC) definitions within the system, a request for a token may contain “scopes” or “audiences” (see [11], [12]) that indicate intent for security-related data exchanges. The authorization server would likely log these token requests, which may increase the attack surface of the system unintentionally. This document does not purport to constitute a complete threat analysis, but it does highlight the kind of analysis that would be necessary when deciding upon an authorization server deployment.

For this flight test, the same authorization server was used for both sensitive and non-sensitive operation data exchanges.

Categories of operations and their sensitivities

Based on real world use cases, three different types of operations in a UTM context have been identified:

1. Non-Sensitive: Data is shared with Commercial USS, Other Federal USS, and within an agency’s own USS
2. Sensitive: Data shared with only other Federal USS, and within an agencies own USS
3. Sensitive-Protected: Data only shared within an agency’s own USS

The type of mission being conducted by the DoD and DHS would determine the amount of information being shared between the agencies and commercial USSs supporting operations in the same airspace. Figure 3 presents the flow of information exchanges with respect to different operational categorizations and associated data sensitivity levels.

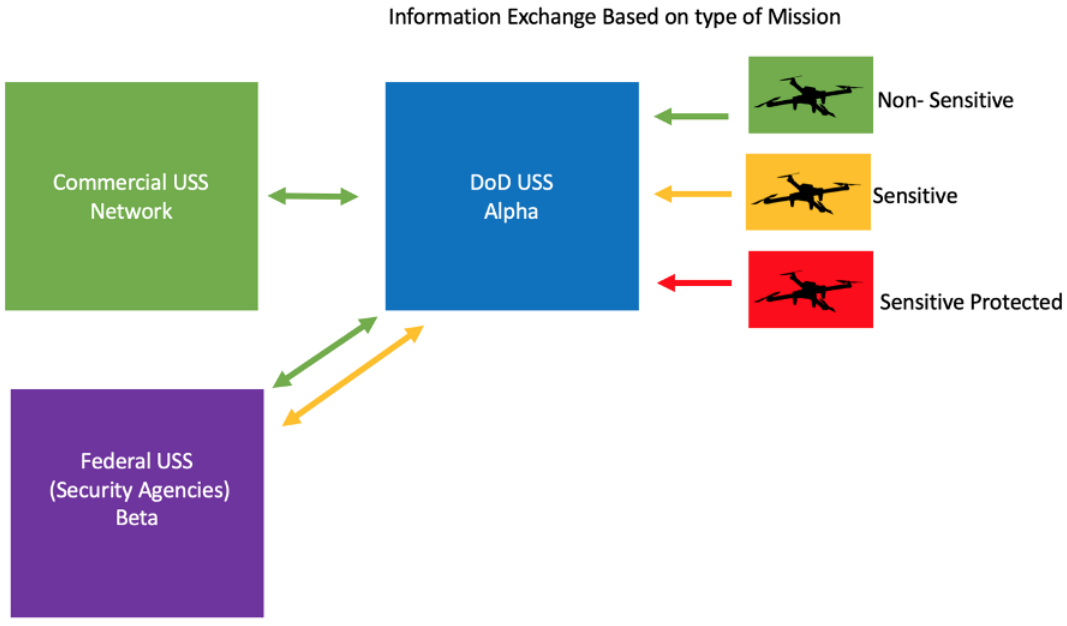

Figure 3. *Flow of information between commercial and security USSs based on sensitivity categorization of missions DoD FUSS-Blue, DHS/Security Agency FUSS-Purple*

Interoperability between security entities

In some use cases, there may be a need for two or more agencies to operate UAS in the same physical area. This requires coordination and situational awareness between the agencies involved. In this type of scenario, each agency's operators would log into their own common operating picture through their own agency's interface. When submitting an operation, the correct data would be shared based on the type of operation and its sensitivity classification. During the flight testing, this example was demonstrated where a DoD operation and DHS operation were submitted near an Air Force base in the same general area. Because both agencies have their own jurisdiction and mission, they can communicate via the COP on how to protect their own assets by identifying nefarious UAS.

Role-Based Access

Based on the DoD and DHS missions, current operations are being explored in CONUS and overseas. The key actors that are at the focus of this study are the Counter-UAS operator, Air Traffic Controller, and UAS operator. The C-UAS operator is responsible for base or location security and has access to C-UAS systems that can detect, identify, and engage nefarious UAS. Currently, the DoD's ATC spend most of their attention and time on managing manned aircraft, with minimal attention focused on UAS operations. By integrating a COP with the aforementioned actors, communication, situational awareness, and decision-making times can be improved.

UTM was designed by NASA originally to follow a RBAC paradigm. The needs of the DoD and DHS can be incorporated into this same paradigm through new definitions for subjects, roles, permissions and other RBAC elements. For more information on how NASA uses RBAC within UTM see [11]. Table 1 introduces elements that were tested during this activity in terms of the identified roles, types of missions certain operators can submit, and the appropriate data shared to the USS network.

Table 1. Role-Based Access Control (RBAC) elements and information access

Operation Type --->	Non-Sensitve Read	Non-Sensitve Write	Sensitive Read	Sensitve Write	Sensitve Protected Read	Sensitve Protected Write	CUAS Feed
Role 1 (UAS Personnel)	Yes	Yes	Yes	No	Yes	No	No
Role 2 (Non-UAS Personnel)*	Yes	No	Yes	No	Yes	No	No
Role 3 (UAS Personnel)	Yes	Yes	Yes	Yes	Yes	No	No
Role 5 (UAS Personnel)	Yes	Yes	Yes	Yes	Yes	Yes	No
Role 7 CUAS Personnel**	Yes	No	Yes	No	Yes	No	Yes
Role 8 Air Traffic Personnel**	Yes	No	Yes	No	Yes	No	Yes

Common Operating Picture

Given that multiple roles have been identified and that there is a critical need for timely communication and a common understanding of the situation, an initial implementation of a Common Operating Picture (COP) was developed to support the flight test and provide early user interaction by participating operators. Part of the structure of the COP is the integration of C-UAS assets that may be available into the overall operational picture. In this case, a Security Federal USS would have a C-UAS asset feed that is only available to the C-UAS operator and the Air Traffic Controller. The asset feed would forward data or tracks obtained from the field to the Federal USS and COP of ATC and the C-UAS operator but would not be available to UAS operators due to the lack of need to know. Figure 4 shows a screenshot of an initial

implementation of the COP's map interface as used in the flight test where active operations are displayed to the user with additional information available through interactive icons. Additional information was available to certain user roles through the Operation and Messages tabs that were accessible from the COP menu (shown on the upper left of Figure 4).

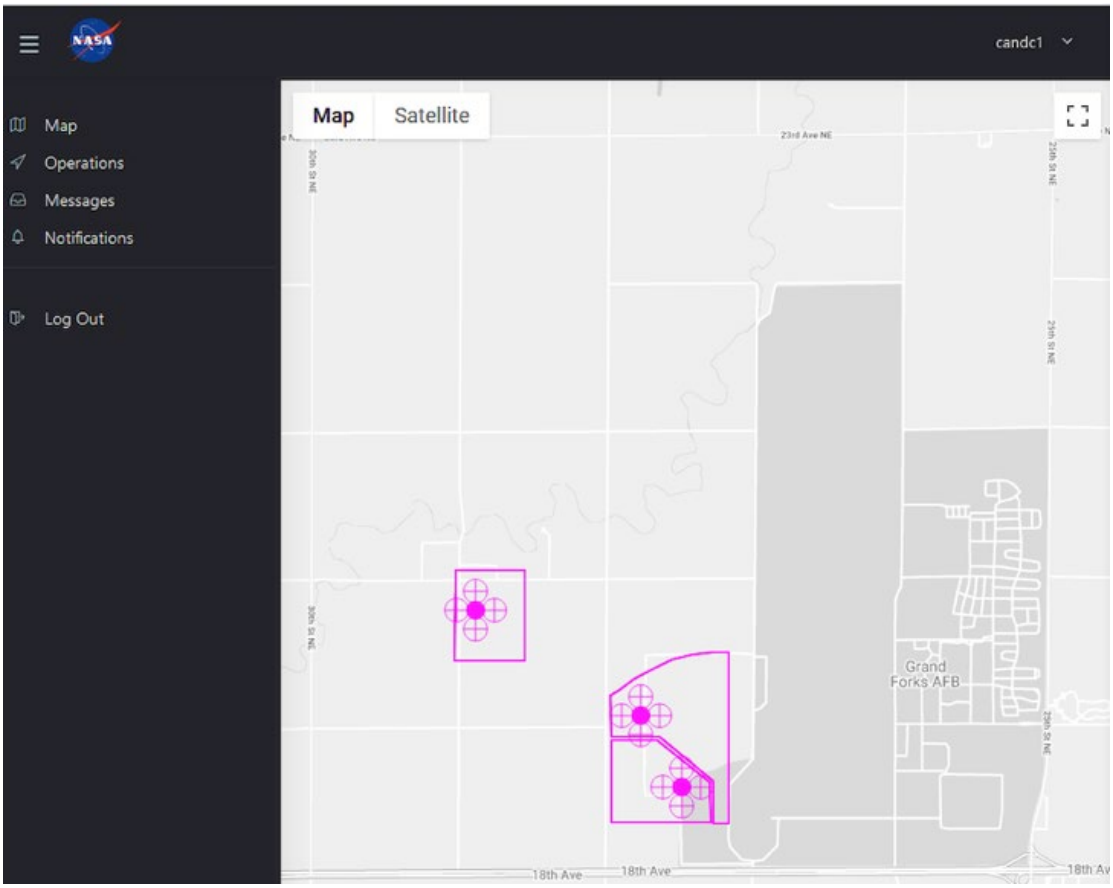

Figure 4. *Screenshot of map display from the COP user interface.*

Tagging and Messaging between Actors

Researchers created a tagging and messaging mechanism for various actors to use when logged into the COP. For this test the concept explored was that each of the roles for C-UAS, ATC, and UAS operator were able to deliver pre-defined messages, queries, and responses to other operators logged onto the common operating picture. Figures 5–7 present the messaging capabilities provided via the COP based on role.

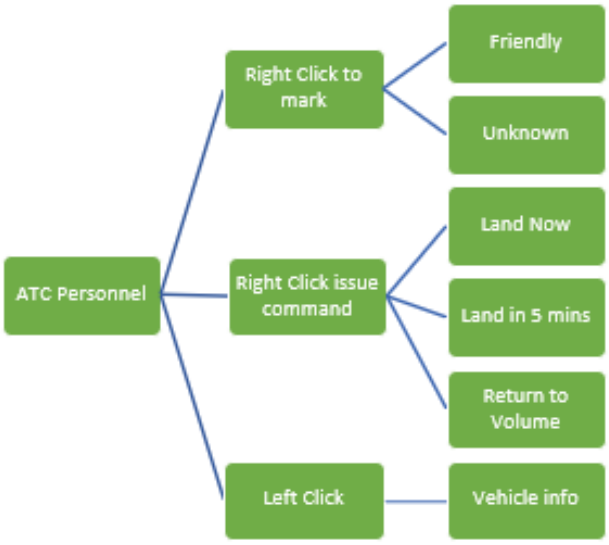

Figure 5. *COP Interaction Capabilities as Tested for the ATC Role*

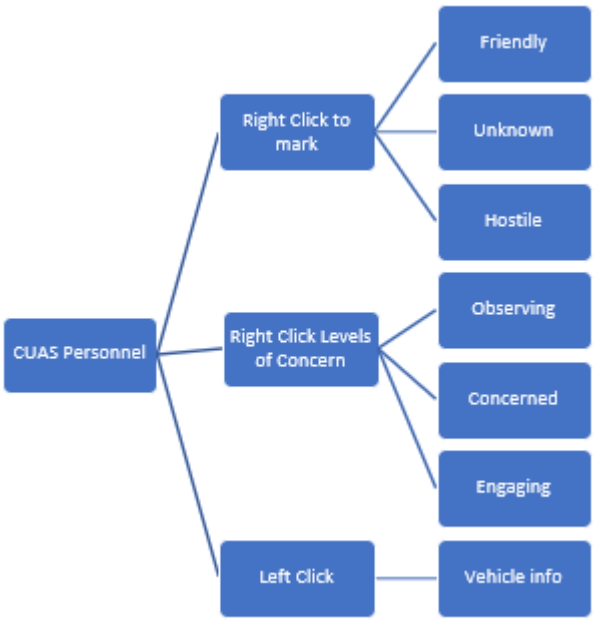

Figure 6. *COP interaction capabilities as tested for the C-UAS role*

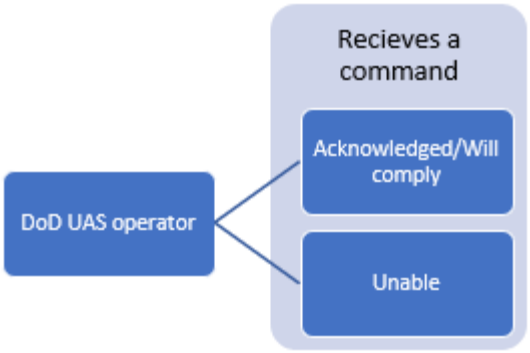

Figure 7. *COP interaction capabilities as tested for the DoD UAS Operator role*

The scenarios incorporated in the flight test provided a number of opportunities for tagging and messaging between operators based on the roles and messaging capabilities afforded by the COP interface. Figure 8 depicts messaging between a C-UAS and ATC operator in the tagging of aircraft and messaging action being taken. Figure 9 presents the interaction between an ATC and UAS operator via COP messaging capabilities as tested.

Figure 8. *Tagging and Messaging between a C-UAS Operator and ATC Personnel via the COP*

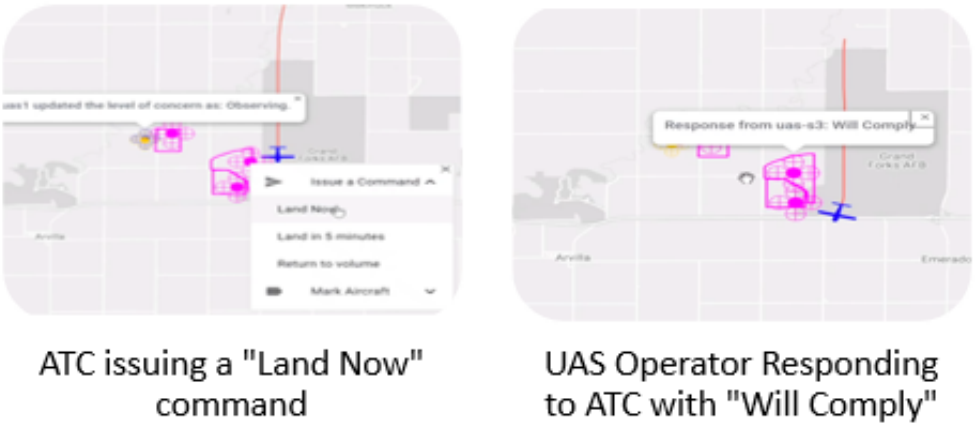

Figure 9. *Tagging and messaging between ATC and UAS Operator via the COP*

C-UAS integration

Military bases, high profile events, and high security areas often have counter UAS systems that assist in detecting UAS operations that may pose a threat to security. Currently these systems are stand alone. However, in order to better provide a C-UAS operator with situational awareness, it is important to integrate existing C-UAS systems and UTM in the form of a Common Operating Picture. For this test, a simulated C-UAS system was connected with the Federal USS, giving the C-UAS operator messaging, alerts, and tagging capabilities. As part of the simulation, a C-UAS radar system was forwarding its feed to a FUSS, which was then displayed as data on the operators' COP. By accessing UTM data, a C-UAS operator can better understand the types of operations occurring in a security area, and the operator can corroborate the UAS tracks picked up by external systems with UTM operations to help inform decision making. For example, in some cases, an out-of-control federal asset could experience a fly away. By utilizing UTM feeds in conjunction with C-UAS and sensor data, the C-UAS operator may choose to not engage their own asset as UAS crews try to regain control of the aircraft; a decision made possible by the access to greater information provided by the COP.

Flight Test Architecture

Building upon the foundations of the concepts and considerations described thus far, NASA, NPUASTS, and Simulyze constructed a flight test architecture that enabled the execution of the demonstration (Figure 10). This architecture enabled the scenario objectives to be tested in the field with the various equipment and UAS that were deployed.

Four USSs were connected to each other through authorization tokens and were each developed to the ASTM standard. The NASA USS was deployed twice as a Federal USS: one for DoD and one for DHS. The CLUE USS was deployed as a Federal partner USS as a passive participant. Simulyze acted as a commercial USS. Additionally, Simulyze had two Supplemental Data Service Providers (SDSPs) connected to the Federal USS: one that ingested the Echodyne Radar and Global Positioning System (GPS) trackers (simulating a C-UAS system picking up UAS) and the other SDSP allowed simulated aircraft to be injected into the scenario. This architecture allowed the research concepts to be integrated and tested in the field and created a foundation for future concept refinement and development of the Federal UTM architecture.

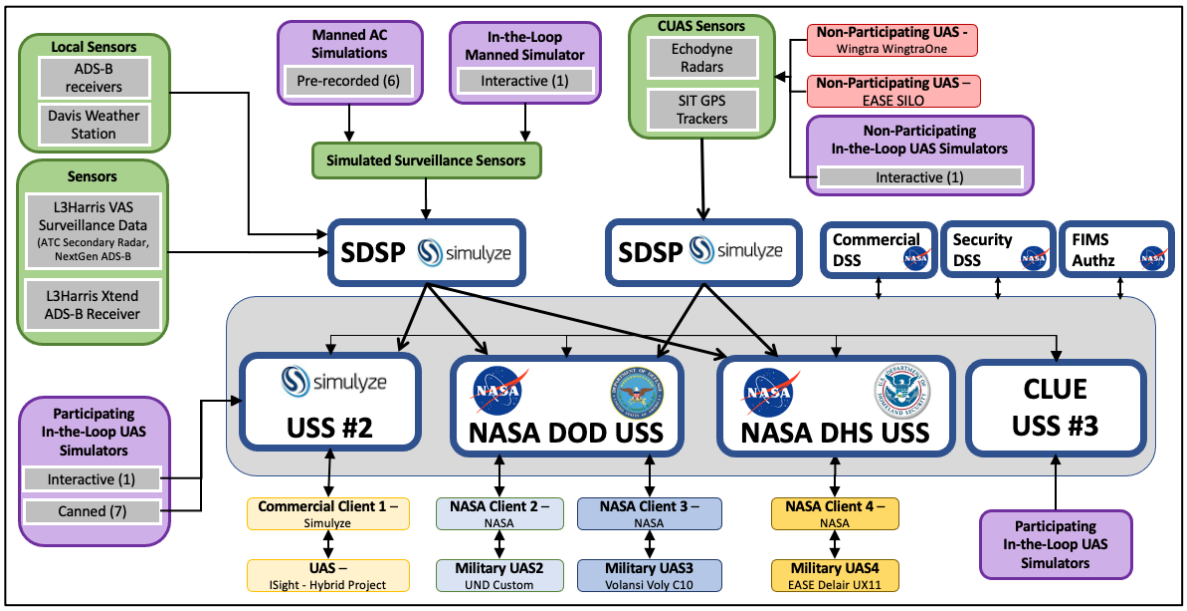

Figure 10. *Flight test architecture*

Flight Test Location and Partners

The flight test was conducted near Grand Forks, North Dakota, adjacent to Grand Forks Air Force Base. During the field test preparations and execution, the Northern Plains UAS test site was responsible for providing a Flight Test Director, site management, logistics, and management of subcontractors for UAS operations and SDSP integration. Simulyze personnel were present at the site for the management of their USS and SDSP components. The CLUE team was also present and stationed in another operations trailer. The objective of the CLUE team was to demonstrate that their Federal USS instance was able to connect with the NASA Federal USS framework and successfully exchange data. Although the NASA and CLUE USSs were labeled as Federal USS, there were distinctions in functions, features, and capabilities. The CLUE USS was modeled after NASA's and focused on connectivity and compatibility with NASA's prescribed USS and DSS requirements to demonstrate the concept of multiple agencies participating in a common environment. The CLUE USS provided simulated traffic in the commercial environment as part of connectivity tests and data exchanges with the primary NASA-provided Federal UTM framework. The NASA USS focused on the key features for federal UTM integration such as role-based access, information sharing of mission data, and the development of a common operating picture to support the diversity of federal stakeholders. All USSs were developed to the ASTM standards as defined at the time of testing.

Flight Test UAS

Six different UAS platforms were used in flight testing. Figure 11 and Table 2 depict the vehicles and provide specifications for each.

Figure 11. *UAS platforms used during the flight test*

Table 2. *UAS Specifications*

UAS	Type	Weight (lbs)	Endurance (min)	Cruise Speed (mph)	Operator	Telemetry Link	RC Link	Quantity	USS
WingtraOne No data push. This will be our non-participating UAS.	VTOL Fixed Wing	9.9	50	34	NPUASTS	2.4GHz	2.4GHz	2	Non-Participating
Custom Hex Pixcube	Multirotor	4.5	20	20	UND RIAS	900MHz	2.4GHz	1	NASA USS
Volansi Voly C10	VTOL Fixed Wing	55	45	50	Volansi	900MHz	2.4GHz	1	NASA USS
EASE SILO	Multirotor	3	20	20	EASE Drones	2.4GHz	2.4GHz	5	Non-Participating
Delair UX11	Fixed Wing	3.1	59	35	EASE Drones	2.4GHz /LTE	2.4GHz	1	NASA USS
Hybrid Project SuperVolo	VTOL Fixed Wing	37.5	300	55	ISight RPV Services	900MHz	2.4GHz	1	Simulyze

Federal UTM Operations Center

While flight operations were taking place at the test site, researchers and security stakeholders were afforded a comprehensive real-time view of the scenarios as they unfolded from a remote location. The Airspace Operations Laboratory, located at the NASA Ames Research Center at Moffett Field, California, acted as an operations center in support of Federal UTM to provide an example framework and environment for higher level mission management functions to the visiting security agencies and support personnel. The Airspace Operations Laboratory specializes in the development and testing of displays and the integration of airspace management systems that is built upon decades of research into ATC and Air Traffic Management. The facility has served as the central operations/mission control center throughout NASA's formal UTM Project technical capability level demonstrations. Figure 12 presents a picture taken from the laboratory during testing with multiple display views and test management support software and material.

Figure 12. *View from the Airspace Operations Laboratory where researchers and stakeholders remotely viewed flight testing in real time.*

Scenario Overview and Results

In order to investigate the systems and approach to Federal UTM integration, three scenarios were developed to address specific areas of interest. These scenarios were designed to test aspects related to DoD Air Traffic Controller and UAS operator interactions, C-UAS operator interactions, and integration of Federal USS to promote a common operating picture. The following are descriptions of each scenario and how they were tested.

Scenario 1

Scenario 1 focused primarily on Air Traffic Controller personnel and their situational awareness with regards to unmanned and manned air traffic. The goal of this scenario was to determine whether the UAS operators on the ground could effectively communicate with DoD Air Traffic Control personnel. During the scenario, ATC personnel issued direct messages and notifications to a DoD UAS operator. Researchers observed how UAS operators responded to digital ATC notifications via response and action (captured in the human factors section). In addition to unmanned traffic, Scenario 1 also called for manned traffic to be injected into the test area, which prompted actions from both the ATC personnel and UAS Operators.

During Scenario 1, three DoD UAS operations were airborne and active as well as one commercial operation. DoD operations 1 and 2 were submitted as Non-Sensitive and DoD Operation 3 was submitted as a Sensitive DoD operation. Based on the test architecture, DoD operations 1 and 2 were shared and subsequently visible on the commercial operating picture

(Figure 13). However, DoD operation 3 was not visible to the commercial operator due to the operation's sensitivity designation (Figure 14). Once the 3 DoD and 1 Commercial operation were airborne, a simulated emergency was injected into the scenario. A simulated medevac helicopter announced to DoD ATC that it was inbound for landing. The Air Traffic Controller projected the flight path of the helicopter to intersect with DoD operation 2 and 3 and therefore requested those operations to close. DoD ATC sent a message via the DoD COP to the UAS operators in the field to close their operations. Both Operators received the message to close. DoD Operation 3 was able to respond to the DoD ATC message by clicking "acknowledge" whereas DoD operation 2 experienced a simulated vehicle command and control malfunction and the operator responded to ATC with "unable".

The DoD Operators on the ground could see the live GPS tracks of all DoD vehicles and the volume of the commercial operation. The simulated helicopter was also depicted in the COP, allowing UAS operators to see the inbound manned traffic (Figure 13). Eventually DoD operator 2 was able to regain control of their UAS and return to their launch point. This created a clear path for the Medevac to land at the air force base without disrupting DoD operation 1 and the commercial operation.

This sequence of events allowed the DoD ATC personnel to efficiently manage the airspace by allowing 2 operations to continue and only affecting 2 others as needed.

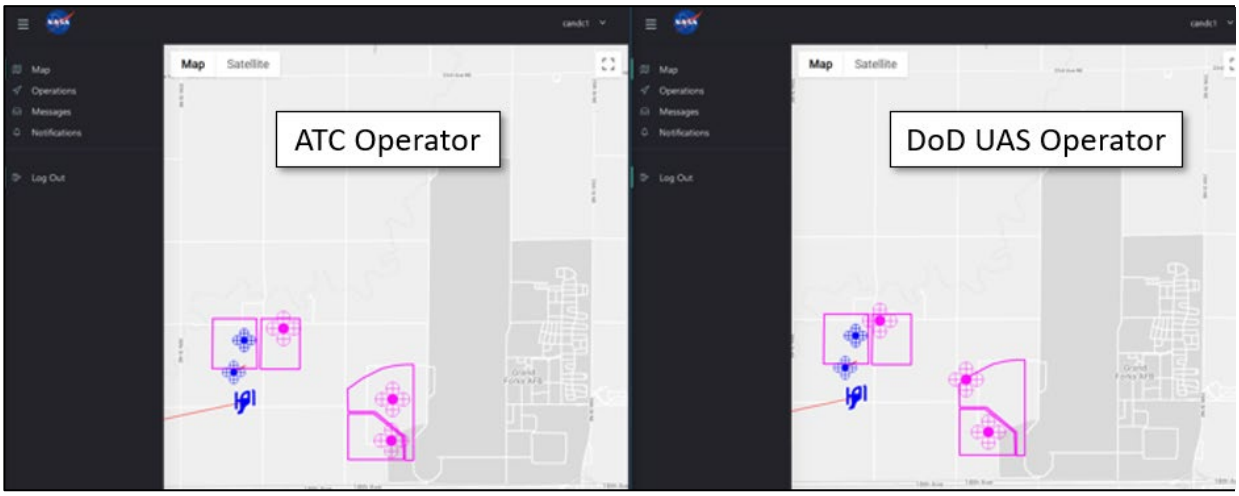

Figure 13. *ATC (left panel) and DoD (right panel) operator views showing common operating picture with shared awareness of simulated medevac flight and UAS operations.*

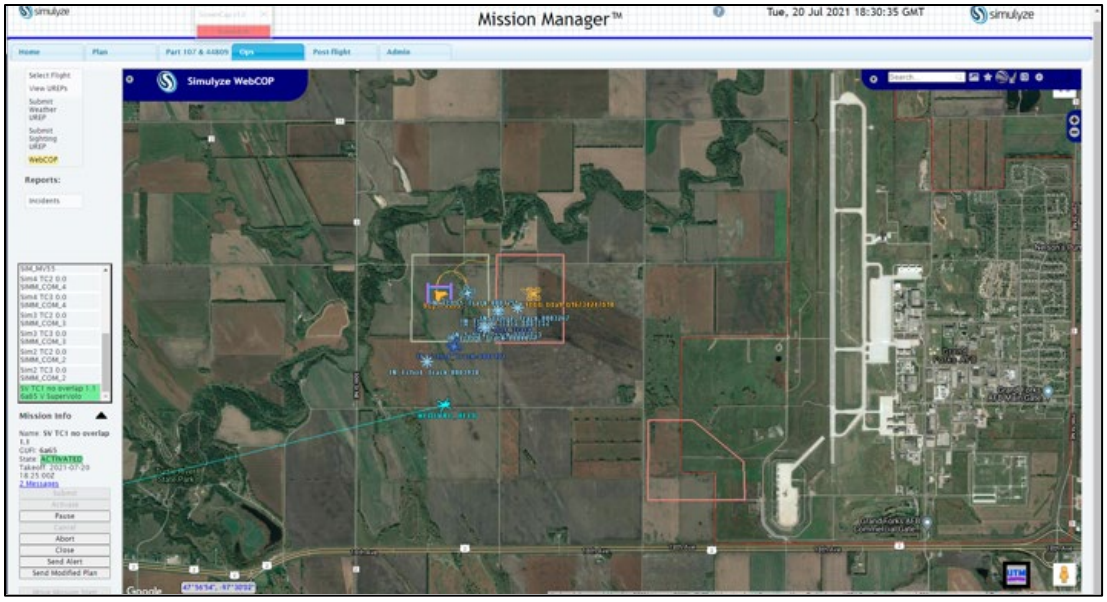

Figure 14. *Commercial operator view. Note the absence of DoD Sensitive operation on the display.*

Scenario 2

Scenario 2 focused on the communication between the DoD ATC and DoD C-UAS operator. The objective was to determine if the DoD ATC and DoD C-UAS personnel could effectively identify and corroborate UAS vehicles by communicating with one another via the COP interface. During this scenario, the DoD ATC and DoD C-UAS operator were presented with categorizations of Friendly, Friendly non-complying, Unknown, and Hostile UAS. The two operators were tasked with identifying the various UAS and communicating with the UAS operator (if it was a DoD operation) or with each other and assign the appropriate operation category (Figure 15). Scenario 2 began with the DoD ATC personnel and the DoD C-UAS operator both physically separated from each other and logged into their respective Common Operating Picture. The Air Traffic Controller could “query” aircraft by right clicking on their associated icon and selecting “Unknown” or “Friendly.” Once the query was selected by an operator the tag would then be displayed on both the DoD ATC personnel screen as well as the DoD C-UAS operator as a notification.

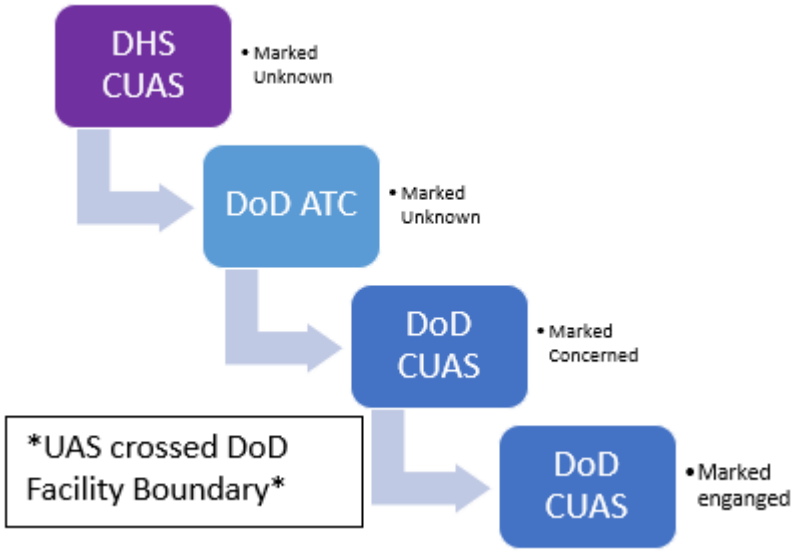

Figure 15. *Flow of communication and annotation of operations between interagency C-UAS and ATC personnel via the COP interface*

The result of Scenario 2 demonstrated that when the DoD ATC and DoD C-UAS operators were physically located at different locations, the COP allowed them to effectively communicate, identify, and in some cases act on a UAS based on the information received. Friendly operations were corroborated and marked, whereas unfriendly operations were observed and engaged in a simulated fashion during the flight testing as well (Figure 16).

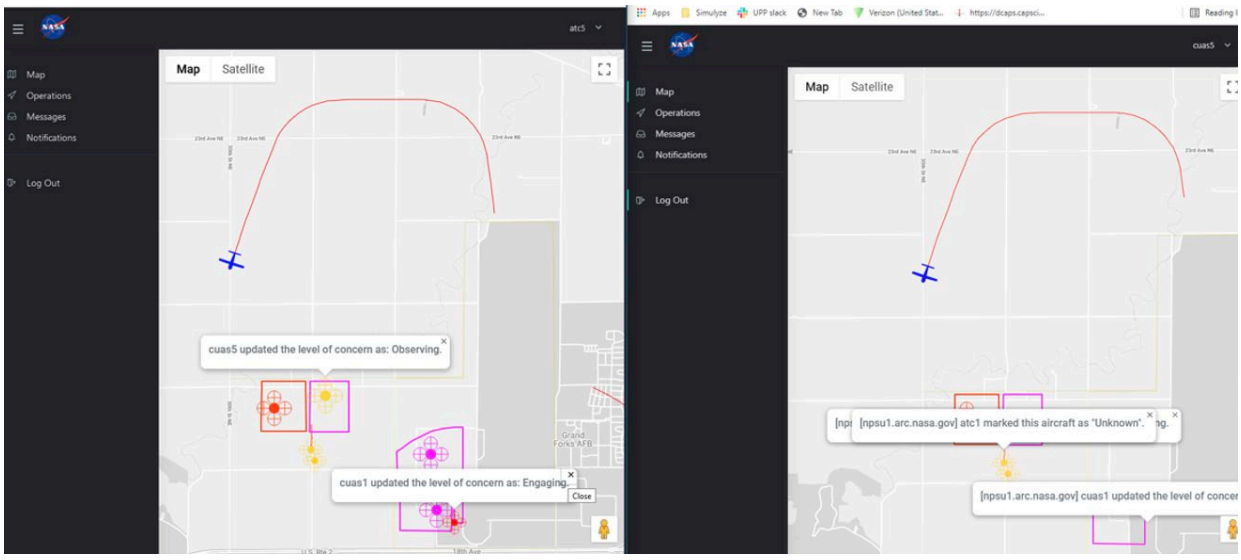

Figure 16. *Screenshot of ATC (left panel) and C-UAS (right panel) COP displays with operation categorization markings displayed and shared via the common platform*

Scenario 3

Scenario 3 built upon Scenario 2 and added another federal USS into the picture. The goal of this scenario was to test the interagency communication between the DoD and DHS operators during a simulated mass gathering event near a DoD Facility. Scenario 3 the integration and interactions between the DoD FUSS, a DHS FUSS, a commercial USS, and the CLUE USS. The DoD ATC, DoD C-UAS, UAS, DHS C-UAS, and associated systems were stress-tested for researchers to assess system performance effects related to the overwhelming amount of notifications and system overload with regards to the amount of data being ingested and shared. During this scenario, the DoD and DHS had specific jurisdictions to operate within. However, the agencies shared sensor data for common situational awareness. The DHS was operating a UAS around a simulated stadium in which the airspace was only authorized for DHS operations. Adjacent to the stadium was a DoD facility, which was controlled by DoD ATC and protected by DoD C-UAS. One interaction highlighted interagency communication in which the DHS C-UAS operator noticed an unknown UAS flying near the protected airspace headed toward the DoD installation. Rather than manually calling the DoD Facility, the DHS C-UAS operator tagged the unidentified UAS as “unknown” via the Common Operating Picture. This prompted a notification on the DoD ATC and DoD C-UAS operators’ respective displays (Figure 17). This notification allowed the DoD C-UAS operator to observe, elevate concern, and/or engage depending on the threat level and proximity to the secure facility. Figure 18 presents the situation view of the commercial operator. Scenario 3 also demonstrated the connectivity and communication between two NASA-prescribed Security FUSS, a Commercial USS, and the CLUE USS.

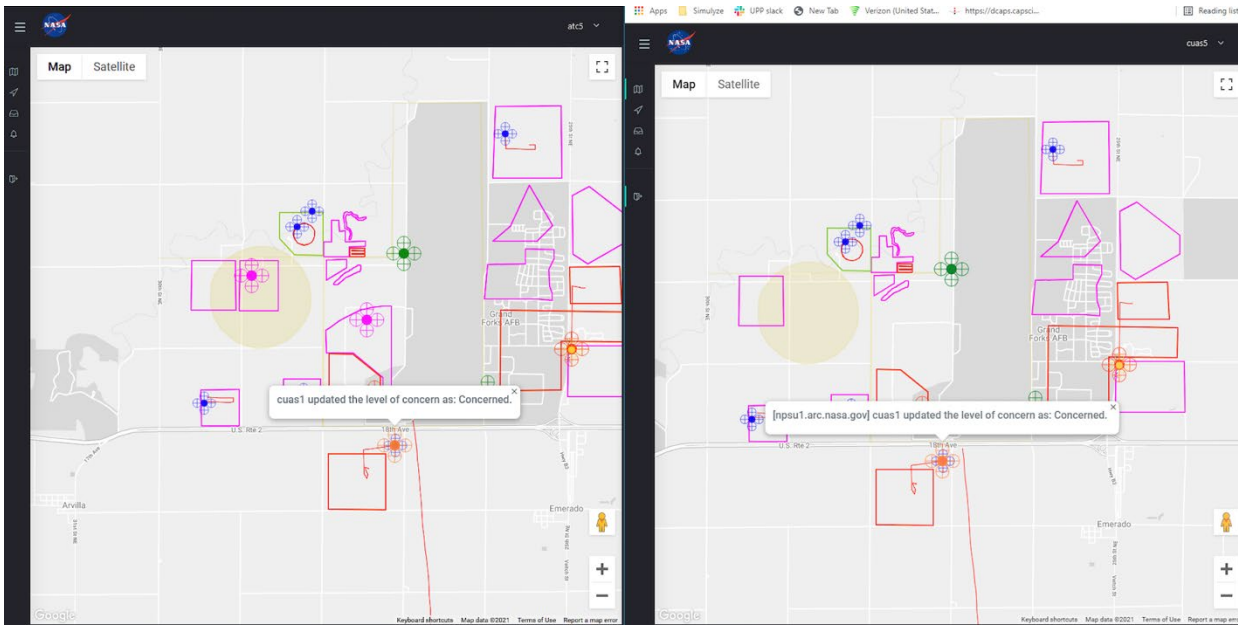

Figure 17. *Interagency coordination between DoD ATC (left panel) and DHS C-UAS Operator (right panel) where level of concern was tagged and communicated (not shown is the same display of information to the DoD C-UAS Operator)*

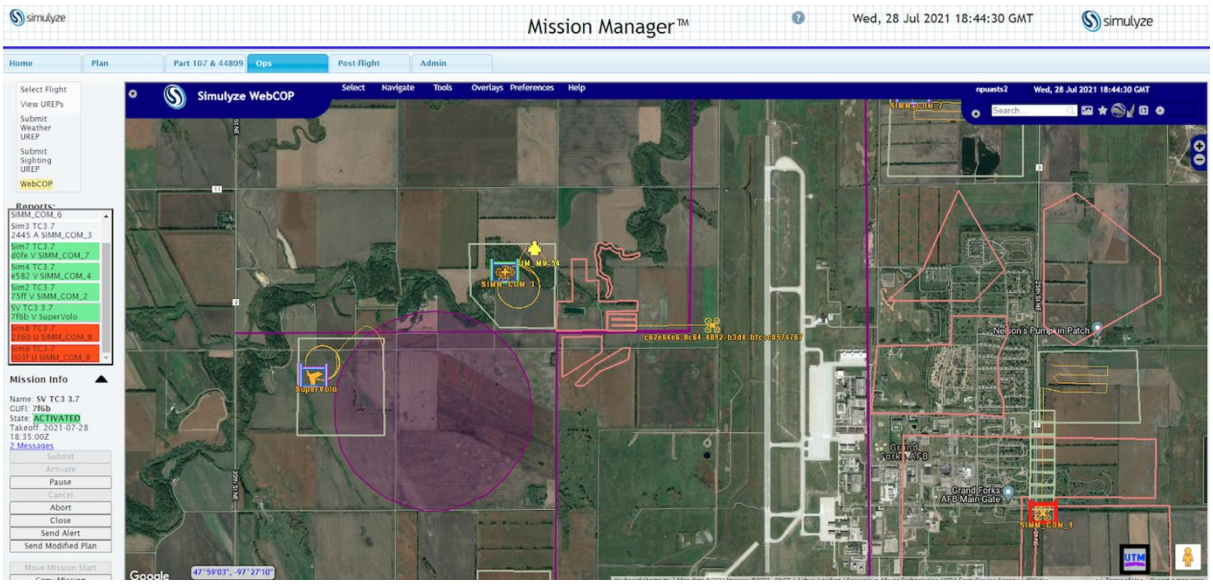

Figure 18. *Simulyze's commercial operator view in Scenario*

Human Factors Results

Human Factors survey responses were gathered from ATC, C-UAS, and UAS Operators as time allowed during data collection days between July 21st and July 26th, 2021. C-UAS and ATC participants received the same set of questions that were suited to their tasks and interface while the UAS Operators received questions that were tailored to their tasks and interface. The surveys were designed to assess the Federal USS functions and features, with a particular focus on the messaging interface that was intended to facilitate coordination between ATC, C-UAS, and UAS operators acting within the same airspace, which necessitated the need for enabling a common operating picture. A total of 28 completed surveys were collected from participants (8 from ATC, 4 from C-UAS, and 16 from UAS operators). The results, analysis, and conclusions from this data are explained below.

Efficiency and Effectiveness

On average, all three types of operators gave the messaging client an efficiency rating of 5.57 and an effectiveness rating of 5.64 out of 7. UAS operators tended to rate the efficiency and effectiveness slightly lower than their ATC and C-UAS counterparts, but all rated the client higher than average for both categories (see Figure 19).

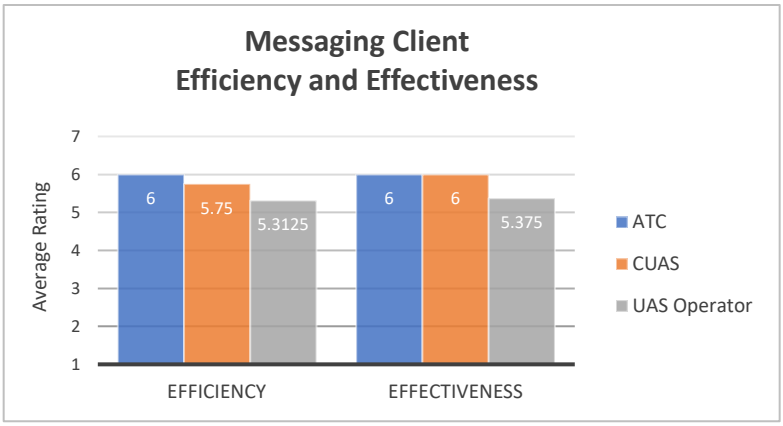

Figure 19. *Prompt: Please rate the efficiency and effectiveness of the messaging client. (1 = very low, 7 = very high; N = 28)*

Usability

All participants were asked to rate the usability of the messaging client based on 8 characteristics: the level of detail, the clarity, conciseness, accuracy, timeliness, and noticeability of information, as well as the usefulness for planning and for decision making. While ATC and C-UAS participants had fairly consistent, above-average ratings (between 5 and 6) for all characteristics, the UAS operators tended to have lower usability scores, particularly in regard to the level of detail and the noticeability of information (see Figure 20).

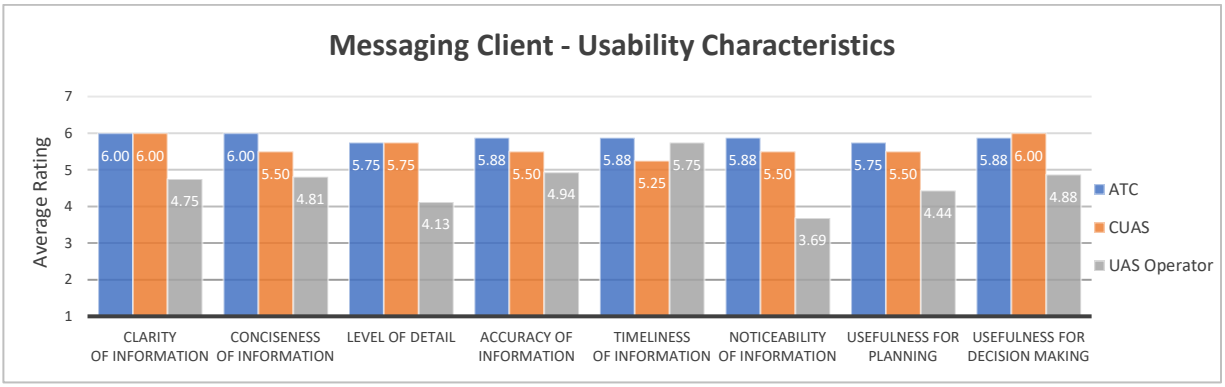

Figure 20. *Prompt: Please rate the messaging client on the following characteristics. (1 = very poor, 7 = very good; N = 28)*

Clutter

Users' perception of the amount and effects of interface clutter were gathered by asking questions about how difficult it was for them to accomplish their tasks due to overlapping elements or the number of elements on the screen. ATC participants reported less difficulty due to overlapping elements and the number of elements (M = 2.38 and M = 2.25, respectively) than UAS operators (M = 3.00 and M = 2.93, respectively). C-UAS participants reported approximately twice the difficulty rating than ATCs for these factors (M = 4.75 and M = 4.33, respectively; see Figure 21). The supplementary comments provided by C-UAS may help understand these participants' ratings. One C-UAS wrote, "there was a point when the ATC was

trying to identify a UAS as “friendly,” but could not because there was too much clutter.” This influenced their perception of the timeliness of information. A C-UAS also wrote, “I think there is still a lot of unnecessary info in the info boxes.”

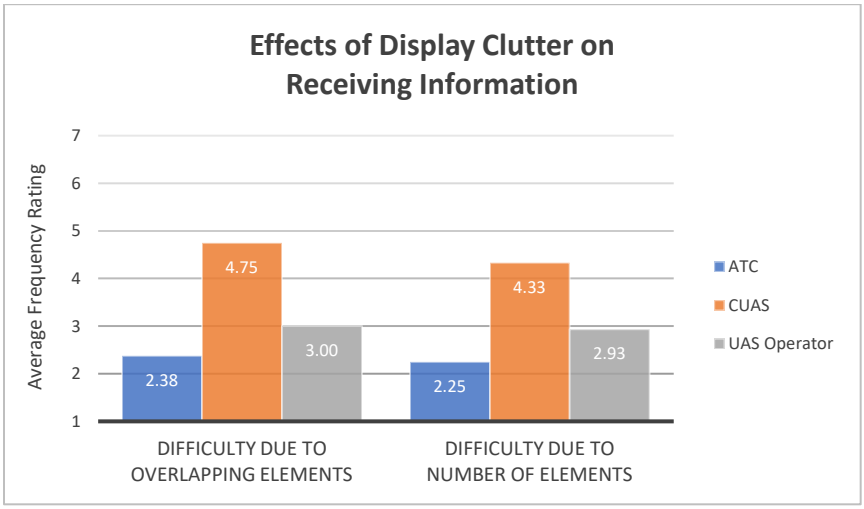

Figure 21. *Prompts: How often did you experience difficulty receiving information due to one element obscuring another (popup boxes, aircraft icons, etc.)? How often did the number of elements on the screen make it difficult for you to find a target or the information you were searching for? (1 = Never, 7 = often; N = 28)*

Aircraft Marking

All participants were asked about aspects of interacting with the messaging client. ATC and C-UAS operators were asked about the factors that contributed to their decision to mark an aircraft in a certain way, the applicability of their marking options, and their understanding of their own and others’ markings. ATC and UAS operators were asked similar questions regarding the actions of issuing a command or a response to a command. When it came to determining how much each component influenced ATCs and C-UAS decisions to mark an aircraft as hostile or friendly, they ranked the factors from having the least to most contribution as altitude (M = 3.90), speed (M = 4.80), magnitude of deviation (M = 5.10), and heading (M = 5.30); however, C-UAS had higher ratings on average than their ATC counterparts (see Figure 22). The name of the USS and the color of the marking were also written in as alternate factors that an ATC considered when deciding to mark an aircraft. One C-UAS remarked that “proximity to buffer zone will always be the biggest indicator for concern.”

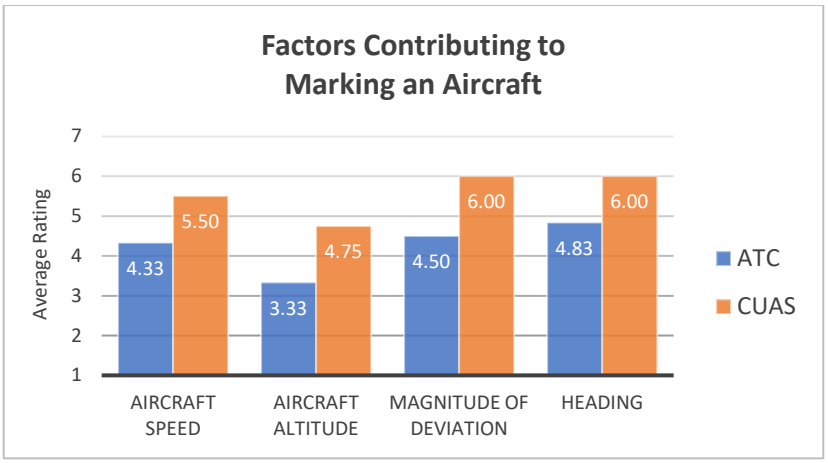

Figure 22. *Prompt: Please rate each factor on how much it contributed to your decision to mark an aircraft as friendly or hostile. (1 = did not contribute, 7 = strongly contributed; N = 12)*

Both ATC and C-UAS participants gave high ratings (*M* = 5.00 and *M* = 4.75) for all three sub-questions regarding the marking purpose, marking option meaning, and marking option sufficiency (see Figure 23). ATC comments for these questions indicated that while they thought the "identified and complying" marking option was useful, they were unsure of rationale for marking an aircraft as "identified and complying" unless it was operating with special conditions outside of the approved volume, and that this case introduced the need for more a free text feature. Another ATC similarly commented that they "Don't know when to change to identified non-complying in the case of other gov agency. Feel like I need more info."

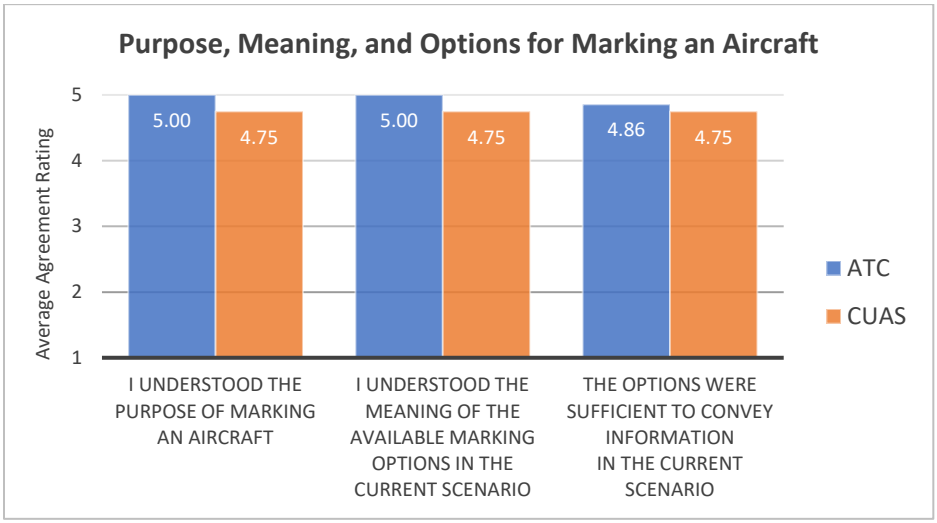

Figure 23. *Prompt: Please indicate how much you agree or disagree with the following statements regarding the action of "Mark Aircraft". (1 = strongly disagree, 5 = strongly agree; N = 12)*

ATC had more variance in their answers to questions about how well they understood or agreed with a C-UAS' aircraft marking decision (Figure 24). Where C-UAS strongly agreed with each statement (*M* = 5.00), ATCs indicated that the C-UAS marking assisted their situation awareness less (*M* = 4.60), they agreed with the C-UAS marking less (*M* = 4.80), they trusted C-UAS markings less (*M* = 4.60), yet they also had less desire for more information. This last result was unexpected but may be an unintended consequence of the question's scale and wording. One ATC commented in writing that "as [they] got busy C-UAS would request info on

aircraft it had already been provided. Recommend history last longer. It only saves last two responses."

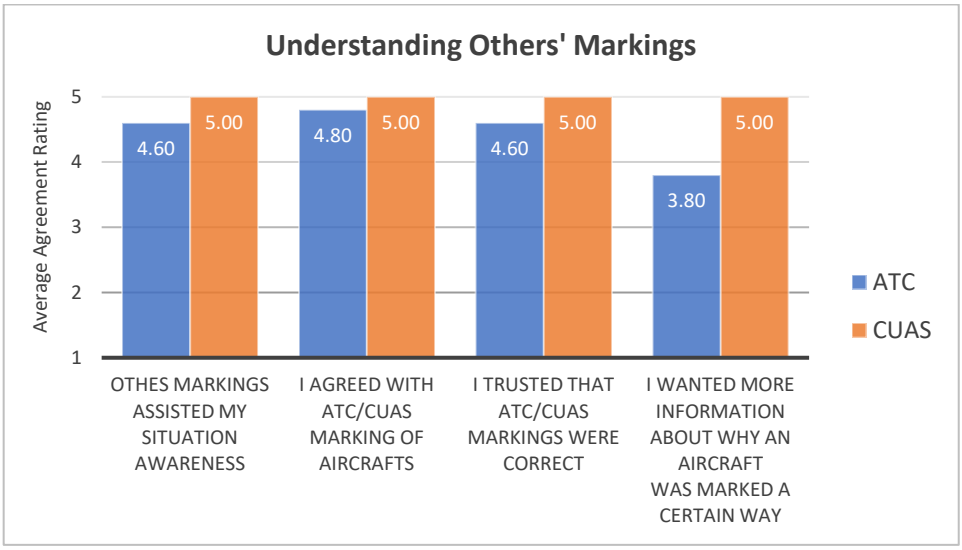

Figure 24. *Prompt: Please indicate how much you agree or disagree with the following statements regarding instances where C-UAS (or ATC) marked an aircraft. (1 = strongly disagree, 5 = strongly agree; N = 12)*

Issuing a Command/Response

When an ATC issued a command to a UAS operator and the UAS operator had to issue a response, the ATC and UAS operators interacted with each other using the messaging interface. Each was asked about the relevance/usefulness of the canned options available to them and whether they understood the meaning of those options. While ATCs always reported that they clearly understood the message options and that those options were sufficient to convey the intended information, UAS operators did not (See Figure 25). UAS operators wrote that they would like for their available options be altered to be more relevant and simple; "simplify command/responses for drop-down box. Commands: "Will Comply" and "Acknowledge" seem redundant and "Simplify responses. i.e., Will comply, yes, no". Table 3 presents additional comments received from the ATC, C-UAS, and UAS Operator participants regarding feedback and suggestions for improvements to the COP interface and its usability.

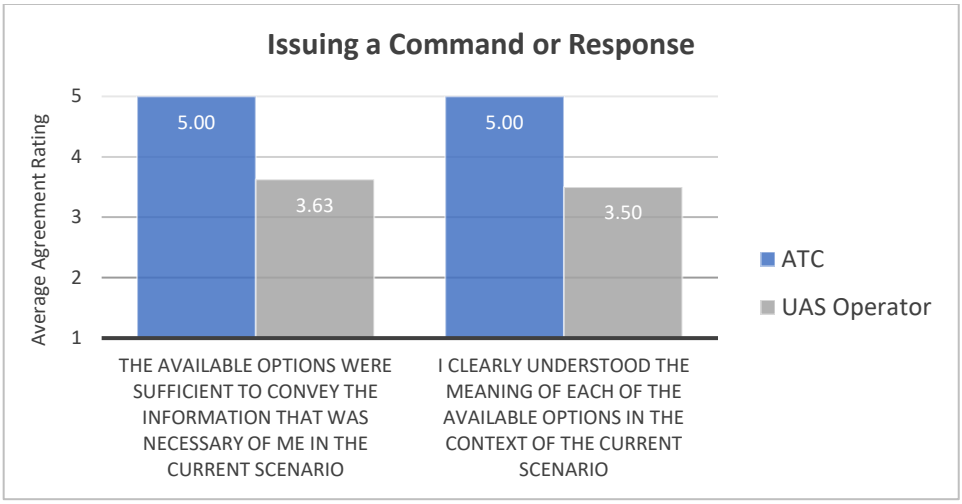

Figure 25. *Prompt: Please rate how much you agree or disagree with the following statements regarding the action of "Issue Command" or "Issue Response". (1 = strongly disagree, 5 = strongly agree; N = 24)*

Table 3. *Additional comments from ATC, C-UAS, and UAS Operators*

Operator Role	Additional Comments
ATC	Scale aircraft icons according to zoom level
	Audio notifications for rogue AC
	Map with perimeter boundaries preferred over satellite
C-UAS	Voice line to ATC
	Textbox with history log
UAS Operator	Audio alerts
	Central message location
	More detail on icons
	More detail in messages
	Simplify response options (e.g., Will Comply, Yes, No)
	Status of other AC in volume
	Increased "Land Now" message saliency
	Eliminate message/pop-up overlaps
	Customizable names in addition to GUFIs

Human Factors Summary

The results from 28 Human Factors surveys gathered from ATC, C-UAS, and UAS Operators during the July 2021 FUSS Flight Tests support the usefulness of a messaging client interface that can facilitate a common operating picture, and responses also provided valuable insights on possible improvements for future iterations. Although the interfaces for each role gave similar capabilities, the underlying tasks and objectives for each role may have influenced their perception of the usefulness and usability of the messaging client.

While both ATC and C-UAS gave high ratings for measures of usability and the efficiency and effectiveness of the client, C-UAS operators reported more difficulty due to the "clutter" of the interface, nearly double the difficulty rating as their ATC and UAS counterparts. Both roles rated the importance of the factors contributing to marking an aircraft, with the most important being heading, then magnitude of deviation, speed, and least important as altitude. C-UAS and ATCs agreed with each other's markings, but both gave additional comments that suggest they

desire more information from the other. C-UAS expressed wrote that they would like for a voice line to ATC and ATC wrote that they wanted their message history to last longer.

Although they rated the efficiency and effectiveness of the client well, UAS Operators gave lower usability scores in 7 of the 8 characteristics, especially for the level of detail and noticeability of information, when compared to ATC and C-UAS participants. UAS Operators also indicated that meaning of the message options was not always apparent or best suited, and they expressed a desire for the options to be more relevant and straightforward.

Conclusion

The objective of this flight test was to determine the functions and features for a Federal USS. More specifically how a UTM COP can assist various users of a Federal USS and other integrated sources of data in decision making and communication. In this particular case, the focus was on interagency communication between UAS, ATC, and C-UAS operators. By creating a baseline FUSS and incorporating role-based access, the integration of C-UAS systems, and air traffic personnel, Federal operators can have better situational awareness and make faster, more optimal decisions. At the conclusion of the flight test, the following objectives were successfully demonstrated:

- ASTM Standard USS-to-USS communication
- Prototype Federal USS
- Role-based Access
- Interoperability messaging between operators
- Situational awareness for operators
- Common Operating Picture

Based on the findings of this test and feedback from operators and stakeholders, NASA has recommended the following for future areas of research:

- Further develop the Common Operating Picture to include additional Federal partners
- Apply more usability research and incorporation of findings to further develop and refine the Common Operating Picture interface
- Continue the exploration of Operations Center requirements for complex operational environments to include displays, visualizations, communications methods, scalable integration of more sensors and data sources, etc.
- Inject manned operations into the scenario where operators can use a mobile device for situational awareness
- Add additional ecosystem features such as LAANC to integrate with a FUSS
- Expand the scope of research to integrate UTM, AAM, and ETM operations for a full capability demonstration
- Collaborate with additional Federal agencies to pursue a more comprehensive National Capitol Region scenario

References

[1] Kopardekar, P., Rios, J., Prevot, T., Johnson, M., Jung, J., and Robinson, J. (2016) Unmanned Aircraft System Traffic Management (UTM) Concept of Operations, 16th AIAA Aviation Technology, Integration, and Operations Conference, Washington, D.C., 13–17 June 2016.

[2] Rios, J., Smith, I., Venkatesen, P., Homola, J., Johnson, M., and Jung, J. (2019) Baseline requirements for providing USS services within the UAS Traffic Management System, NASA Technical Memorandum, NASA/TM-2019-220376.

[3] Aweiss, A., Owens, B., Rios, J., Homola, J., Mohlenbrink, C. (2018) Unmanned Aircraft Systems (UAS) Traffic Management (UTM) National Campaign II, AIAA SciTech Forum. January 8–12, 2018, Kissimmee, FL.

[4] ASTM International. New Specification for UAS Traffic Management (UTM) UAS Service Supplier (USS) Interoperability, ASTM F38.02 WK63418 Working Group. https://www.astm.org/f3548-21.html [retrieved on October 13, 2022]

[5] Rios, J., Aweiss, A., Jung, J., Homola, J., Johnson, M., and Johnson, R. (2020) Flight Demonstration of Unmanned Aircraft System (UAS) Traffic Management (UTM) at Technical Capability Level 4, AIAA Aviation Forum 2020.

[6] Aweiss A. et al. (2019). Flight Demonstration of Unmanned Aircraft System (UAS) Traffic Management (UTM) at Technical Capability Level 3. IEEE-DASC, September 8–12, 2019, San Diego, CA.

[7] Federal Aviation Administration. (2020) Unmanned Aircraft Systems (UAS) Traffic Management (UTM) UTM Pilot Program (UPP), UPP Phase 1 Technical Report, Version 1.0. https://www.faa.gov/uas/research_development/traffic_management/utm_pilot_program/media/UPP1_Technical_Report_version2.0.pdf [retrieved on March 7, 2022]

[8] Federal Aviation Administration. (2021) Unmanned Aircraft Systems (UAS) Traffic Management (UTM) UTM Pilot Program (UPP), UPP Phase 2 Technical Report, Version 1.0. https://www.faa.gov/uas/research_development/traffic_management/utm_pilot_program/media/FY20_UPP2_Final_Report.pdf [retrieved on March 7, 2022]

[9] The Linux Foundation. (2022) InterUSS Platform. https://interussplatform.org/ [retrieved April 21, 2022]

[10] [The Linux Foundation. (2022) DSS Github Repository. https://github.com/interuss/dss [retrieved April 21, 2022]

[11] Hardt, D. (2012) The OAuth 2.0 Authorization Framework. RFC 6749, DOI 10.17487/RFC6749, October 2012, https://www.rfc-editor.org/info/rfc6749 [retrieved on April 21, 2022]

[12] Rios, J., Smith, I., and Venkatesen, P. (2019) UAS Service Supplier Framework for Authentication and Authorization. NASA Technical Memorandum, NASA/TM–2019–220364, https://ntrs.nasa.gov/api/citations/20190032004/downloads/20190032004.pdf [retrieved on April 21, 2022]

Acronyms/Abbreviations

AAM	Advanced Air Mobility
AIAA	American Institute for Aeronautics and Astronautics
ASTM	Formerly American Society for Testing and Materials
ASTM	Formerly American Society for Testing and Materials
ATC	Air Traffic Control
BVLOS	Beyond Visual Line of Sight
C-UAS	Counter-Unmanned Aircraft Systems
CLUE	Collaborative Low-Altitude UAS Integrated Effort
CONUS	Contiguous United States
COP	Common Operating Picture
DASC	Digital Avionics Systems Conference
DHS	Department of Homeland Security
DoD	Department of Defense
DSS	Discovery and Synchronization Service
ETM	Upper E Traffic Management
FAA	Federal Aviation Administration
FUSS	Federal UAS Service Supplier
GPS	Global Positioning System
IEEE	Institute of Electrical and Electronics Engineers
LAANC	Low Altitude Authorization and Notification
M	Mean/Average
N	Sample Size
NPUASTS	Northern Plains UAS Test Site
RBAC	Role-Based Access Control
SDSP	Supplemental Data Service Provider
STI	Scientific and Technical Information
TM	Technical Memorandum
UAS	Unmanned Aircraft Systems
UPP	UTM Pilot Program (FAA)
US	United States
USS	UAS Service Provider
UTM	Unmanned Aircraft Systems (UAS) Traffic Management
VTOL	Vertical Takeoff and Landing

\